Mathematical Modeling of Physical and Engineering Systems in Quantum Information

Horace P. Yuen
Department of Electrical Engineering and Computer Science,
Department of Physics and Astronomy,
Northwestern University, Evanston, IL, 60208,
Email: yuen@eecs.northwestern.edu

February 1, 2008

Abstract

Several concrete examples in quantum information are discussed to demonstrate the importance of proper modeling that relates the mathematical description to real-world applications. In particular, it is shown that some commonly accepted conclusions are not adequately supported by their purported justifications in the logical manner required.

1 Introduction

This paper describes the major part of my talk at the 2006 QCMC meeting. (The rest on unconditionally secure quantum bit commitment are included in my writeup in this volume for my poster paper.) It may be viewed as a concrete elaboration of my points on the role of mathematical modeling and rigor in real-world applications discussed in [1] and [2]. In the context of quantum information, such consideration is especially important and indispensable, if we ever want to develop a true quantum information technology. There are three main points in the following that are presented in three sections:

(i) Entropy or mutual information that the attacker possesses on a generated key is not a good quantitative measure of security in real cryptosystems.

(ii) Given the entropy criterion, there is no security proof, unconditional or just limited ones that include all currently feasible attacks, for any experimental BB84 system.

(iii) Loss is a major limiting factor on many quantum information systems that has not been properly dealt with theoretically.

These assertions may appear startling to many, as they are contrary to the "accepted opinion", if I may say, of much of the quantum information community. However, at this point of writing, I believe they are incontrovertible truths. I hope this is substantiated in the following.

2 Performance Criteria and Security Guarantee

Let us consider the issue of security measure on the generated key K_g in a quantum key generation (QKG) system. Eve's Shannon entropy $H_E(K_g)$, or equivalently her mutual information $I_E = |K_g| - H_E(K_g)$, is the most commonly used measure. If Eve's knowledge of K_g is bit by bit, the binary entropy of a bit is in one-one correspondence with Eve's bit error rate. However, in general Eve has bit-correlated information on K_g, and we may ask: What is the concrete security guarantee provided by having $I_E \leq \epsilon$ for a given level ϵ? The problem arises because I_E or H_E is a theoretical quantity with no operational meaning automatically attached. In standard cryptography, this issue does not arise because fresh key generation is considered impossible [3-5] and was never attempted, while security of other cryptographic functions is based on computational complexity.

In ordinary communications, the operational significance of the entropic quantities is given through the Shannon source and channel coding theorems, which relate them to the empirical quantities of data rate and error rate. But what is the corresponding empirical security guarantee in cryptography? This issue was *not* addressed by Shannon in his classic cryptography paper written at about the same time as his classic information and communication theory papers. It was not addressed by anybody else since.

It is clear that entropy is just a one-number representation of a whole probability distribution. All questions of security could be answered by knowing the complete distribution, which I would like to call Eve's error profile. Let $p_i = p_E(K_g|Y^E S^E)$, where K_g is an n-bit string, Y^E is Eve's observation, S^E is her total side information, be ordered $p_1 \geq \cdots \geq p_N, N = 2^n$. Thus, p_1 is Eve's maximum probability of guessing K_g correctly with her information. As a one-number representation of p_i, p_1 is of special importance because it must be sufficiently small for a meaningful security guarantee. Even for moderate $|K_g| \sim 10^2 - 10^3$, it appears that $p_1 \sim 2^{-20}$ may not be small enough for many applications, while $p_1 \sim 2^{-10}$ would be a disastrous breach of security.

Generally, if Eve can try m different possible K_g to break the cryptosystem, the first m p_i are the relevant numbers to determine any quantitative level of security. For N possible trials, the trial complexity $C_t = \sum_{i=1}^{N} i \cdot p_i$ which is the average number of trials Eve needs to succeed, is a meaningful measure of security. The number p_1 itself is operationally meaningful, and is in fact the most suitable measure if a single number has to be used in lieu of the whole p_i.

To illustrate this and the problem of I_E, we observe that given $p_1 \leq 2^{-l}$ for some l, we have $C_t \geq (2^l + 1)/2$ and $I_E \leq n - l$ [3]. In the worst case p_i, one has [3],

$$p_1 \sim 2^{-l} \qquad \text{for} \qquad I_E/n \sim 2^{-l}. \tag{1}$$

Thus, if Eve has 10^{-3} bit of information per bit of K_g, it is possible that her $p_1 \sim 2^{-10}$. This possibility arises from the possible correlation between the bits of K_g that is reflected in Eve's information on the whole K_g. The p_i that gives one deterministic bit of information to Eve out of $|K_g| = 10^3$ in the above example is the best, not the worst case, for the users. It is not a meaningful procedure to average Eve's p_1 or other measure over the possible p_i given a fixed level of I_E, because there is a definite p_i that Eve has for the given cryptosystem.

Thus, to ensure proper security via I_E, one must have l sufficiently small in $I_E/n \sim 2^{-l}$. It is difficult to ensure exponentially small I_E in an entropic analysis of an experimental system. In fact, $I_E/n \sim 2^{-10}$ is considered very good in current experimental BB84 schemes, with 0.1% information leak per bit after error correction and privacy amplification [6]. But as analyzed above, this does not rule out the possibility of a disastrous breach of security. This exponential problem persists if the Kolmogorov distance $\delta(p, p^0)$

between p_i and the uniform distribution p^0 is used in lieu of I_E.

It is possible to use privacy amplification algorithms to guarantee exponentially small I_E, but the known result [7] from Renyí entropy is always loose by a factor of 2 in the exponent for bounding p_1. In addition, Renyí entropy is difficult to deal with quantitatively. There is no example in quantum cryptography in which it has been usefully bounded in the finite n case, other than the i.i.d. situation which does not cover all the currently feasible attacks. On the other hand, many theoretical results in information and communication theory yield directly the exponential behavior of p_1. In this connection, it is important to observe that $l = \log p_1$ is the true limit on the number of fresh key bits generated in a QKG or classical key generation system. Thus, I recommend that p_1 be employed as the security measure in both theoretical and experimental cryptosystem studies.

Here I would like to mention the following problem of BB84: Since Eve can break the system completely by a man-in-the-middle attack if she guesses correctly the message authentication key K_m needed for the public channel, what is the meaning that a much longer fresh key than $|K_m|$ is still generated?

3 BB84 Security Proofs

The assertion I would like to make now is that no complete QKG protocol has been given with quantified security level that is proved unconditionally secure in a realistic setting including inevitable loss and noise. By a *complete protocol* I mean one which has all the steps specified that can be implemented in a real system and which goes all the way to yield a final generated key K_g that has proven security, say $I_E \leq \epsilon$ for a fixed security level ϵ. Such a complete protocol is needed by an experimentalist to implement a cryptosystem with quantified security, granting here that I_E is used as a security measure. Such a quantified "secure" cryptosystem is what we need to produce to substantiate the claim that we have a "secure" QKG system while there is no comparable provenly secure classical cryptosystem.

This requirement implies that all asymptotic analysis and random coding existence proofs with no finite code specified are not sufficient for a real cryptosystem that always has a finite bit length and that requires explicitly specified protocol steps. Indeed, even if a code is specified, it is not "realistic" when the decoding cannot be carried out in polynomial time. This is especially the case in view of the fact, to be shown elsewhere, that exponen-

tial inefficiency can be utilized to generate fresh key via exponentially small probability of success.

There are as yet only two papers with unconditional security claim on the finite realistic protocols presented that include the effect of noise. In [8], the code is not specified and it is not clear if a code, especially one with polynomial-time decoding algorithm, can be found in a typical experimental parameter region. In [9], the final quantitative result is derived under approximation without rigorous bounds. Both [8] and [9] do not include all possible attacks in a system with transmission loss, as is the case for every security proof given thus far.

The typical loss of linear attenuation is inevitable and usually considerable in an optical system. Its effect on the security of BB84 or Ekert type cryptosystem has never been rigorously determined, while it is accepted by many in the "community" that it only affects the throughput of a single-photon BB84 system but not its security. That this has *not* been established by a proper analysis is readily seen from the fact that the qubit model is not applicable to the situation where the transmission medium is lossy. If only the detector is lossy, but Eve is assumed not able to manipulate it, a good assumption in most cases, the qubit model holds for transmission. If the line is lossy, and Eve is assumed capable of introducing an alternative lossless medium, there are additional attacks she could launch on single-photon BB84 similar to the case of coherent-state or multi-photon BB84. Even at the individual attack level, she could launch an approximate probabilistic cloning attack similar to the unambiguous state discrimination attack in the multi-photon case.

With probabilistic cloning, it is possible to clone nonorthogonal linearly independent states with a nonzero, and of course nonunity, probability [10]. Similarly, it may be possible to approximately n-clone any set of states with a nonzero probability and fidelity larger that that obtainable with unity probability. This possibility has been explicitly demonstrated [11]. By adjusting the probability of success for a given loss level, Eve could launch such an attack on single-photon BB84 without being detected. If the resulting fidelity in a 2-clone is higher, Eve's attack becomes more powerful in the lossy case.

This possibility has not been analyzed in the literature, although for individual attacks it can be shown that the fidelity cannot be increased in this way [12]. However, this already shows that a 3-level model of a qubit in loss is necessary to represent the physical situation, so that all possible attacks by Eve are accounted for in a joint attack. Actually, an infinite-

dimensional multimode model should be used. This analysis is currently lacking. In particular, the use of decoy states [13] in multi-photon BB84 in loss does not solve the security problem of such sources in loss, because at best the problem of single-photon BB84 in loss remains.

Actually, I believe there are several problems in the current proofs of BB84 security that make the validity of various arguments quite questionable. They will be addressed elsewhere. A lot of these problems center around the issue of how one may be able to make rigorous assertions on a multi-correlated system by examining just one copy. It also appears to me that only symmetrized joint attacks are included in the current proofs. It has not been shown why unsymmetrical attacks, especially adaptive ones, could not do better. These problems disappear in the case of individual attacks. However, for such attack, the problem of fully accounting for the side information that can be exploited in just collective classical processing is difficult, and many errors on this issue in the literature can be found [14]. On the other hand, there is no such problem in the KCQ (Keyed Communication in Quantum Noise) approach [3, 15].

Note added: The issues of Sections 2 and 3 are being addressed by M. Hayashi and applied to the experiment of A. Tomita. The security and efficiency analysis of BB84 including especially message authentication will be presented by our group shortly.

4 Loss in Quantum Metrology and Quantum Computation

Loss is a major limiting factor on the quantum effects obtainable in a physical system, which is well-known in quantum optics in the case of squeezing [16] and especially superposition of "macroscopic states" [17, 18]. Recently, it has been proposed that the NOON state $|\psi\rangle = \frac{1}{\sqrt{2}}(|N\rangle|0\rangle + |0\rangle|N\rangle)$ for number state $|N\rangle$ could lead to improved interferometric measurements with , e.g., a phase resolution $\Delta\phi \sim 1/N$ instead of the $\sim 1/\sqrt{N}$ obtained with coherent states. They would find many applications under the heading of "quantum metrology". Actually, squeezed states alone on a single mode would lead to such improvement without entanglement, which is the optimum value

obtainable for a fixed N [16]. Also, the state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|N\rangle|N-1\rangle + |N-1\rangle|N\rangle) \tag{2}$$

leads to similar improvement [19] as the NOON state $|\psi\rangle$, and can be more closely generated by optical parametric processes.

Superposition of macroscopic states is "supersensitive" to loss. I have re-emphasized the significance of this phenomenon in quantum information [2, 20]. Consider the state $\frac{1}{\sqrt{2}}(|n_1\rangle|n_2\rangle + |n_2\rangle|n_1\rangle)$ for number states $|n\rangle$, with ρ the corresponding density operator. Let ρ' be the incoherent superposition $\rho' = \frac{1}{2}(|n_1\rangle|n_2\rangle\langle n_1|\langle n_2| + |n_2\rangle|n_1\rangle\langle n_2|\langle n_1|)$. If the system is in typical linear loss with transmittance η, it is readily computed that the trace distance is [20]

$$\|\rho - \rho'\|_1 = 2\eta^{n_1+n_2}. \tag{3}$$

Thus, for large $n_1 + n_2$, $\|\rho - \rho'\|_1 \sim 2e^{-1}$ and the system effectively decoheres with the loss of one photon. For a large N NOON state, a fractional loss of $1/N$ would already destroy the quantum effect responsible for the $\Delta\phi$ improvement. Furthermore, (3) shows qualitatively that the entanglement effect responsible for the improvement of any usual performance criterion is wiped out with a tiny loss. This should remain true for any other entanglement of macroscopic states. The coherent state case is also worked out in ref. [20].

I believe a similar supersensitivity obtains in a long multi-qubit entanglement for quantum computation, which cannot be removed by fault-tolerant quantum computing or "quantum leak plumbing". The reason is that the terms in a long superposition of many qubits also contain many quanta, which would become supersensitive in the presence of loss similar to the NOON state. The situation cannot be rectified by fault-tolerant qubits which are themselves lossy. Also, quantum leak plumbing disturbs the system in an unpredictable way even if no leak is found. To my knowledge, this whole issue has not been properly treated theoretically in the literature. While linear loss is significant in all current experimental quantum computation schemes, there are many other theoretical schemes in which such loss can be made negligible. However, the moral I would like to draw here is that we should incorporate all the small but perhaps ultimately significant perturbations in the theoretical study of quantum information systems, and one should not believe that a system would do what it is designed for without

such perturbations and small details fully taken into account in the system model.

5 Conclusion

There is currently a huge divide between theory and experiment on quantum information systems, even just on a small scale. I believe this arises also from inadequate modeling of the system as in the large scale case discussed above. In cryptography, there is the further complication that security guarantee has to be obtained with mathematical rigor, assuming the model is complete and correct. It is possible to show that a cryptosystem is insecure by an experiment or a simulation, but it is not possible to *prove* a cryptosystem secure by such means or by other qualitative reasoning. This point I made in [1] comes in full force for security guarantee. We should be extra careful in our modeling and proofs of quantum cryptographic systems. Finally, there is the question whether any useful concrete system can be built for a realistic application if it is so model-sensitive as in the BB84 case, an issue we have not discussed but is widely known.

6 Acknowledgement

I would like to thank Eric Corndorf, Won-Young Hwang, Max Raginsky, and especially Ranjith Nair on many useful discussions on the topics of this paper, which was supported by DARPA under grant F 30602-01-2-0528 and AFOSR under grant F A 9550-06-1-0452.

References

[1] H.P. Yuen, in *Quantum Communications, Computing and Measurement*, ed. by O. Hirota et al, Plenum, New York, pp. 17-23, 1997.

[2] H.P. Yuen, in Mathematical Sciences (in Japanese), no. 508, Oct 2005, pp. 35-40; also in quant-ph 0510069, 2005.

[3] H.P. Yuen, quant-ph 0311061.

[4] H.P. Yuen, R. Nair, E. Corndorf, G. Kanter, and P. Kumar, Quantum Inform. and Comp. 6 (7) p. 561, 2006; also quant-ph 0509091.

[5] R. Nair, H.P. Yuen, E. Corndorf, T. Eguchi, and P. Kumar, Phys. Rev. A 74, p. 052309, 2006; also quant-ph 0603263.

[6] A. Tomita, talk and booth presented at QCMC 2006.

[7] C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. IT 41 (1995) pp. 1915-1922.

[8] H. Inamori, N. Lutkenhaus, and D. Mayers, quant-ph 0107017.

[9] M. Hayashi, Phys. Rev. A 74, p. 022307, 2006.

[10] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. 80, pp. 4999-5002 (1998).

[11] J. Fiurasek, Phys. Rev. A 70, p. 032308 (2004).

[12] R. Nair, private communication, Sep 2006.

[13] W.Y. Hwang, Phys. Rev. Lett. 91, p. 057901, 2003.

[14] K. Yamazaki, R. Nair, and H.P. Yuen, 'Problems of the CASCADE Protocol and Renyi Entropy Reduction in Classical and Quantum Key Generation', in this volume; also quant-ph 0703012.

[15] H.P. Yuen, 'Direct Use of Secret Key in Quantum Cryptography' in this volume; also quant-ph 0603264.

[16] H.P. Yuen, in *Quantum Squeezing*, ed. by P.D. Drummond and Z. Ficek, Springer Verlag 2003, pp. 227-261.

[17] A.O. Caldeira and A.J. Leggett, Phys. Rev. A 31, 1059-1066 (1985).

[18] D.F. Walls and G.J. Milburn, Phys. Rev. A 31, 2403 (1985).

[19] H.P. Yuen, Phys. Rev. Lett. 56, 2176 (1986).

[20] H.P. Yuen, in Proceedings of the 1995 Squeezed States Conference, NASA Conference Publication 3322, pp. 363-368 (1996).